UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v.

HAMID AKHAVAN and RUBEN WEIGAND,

Defendants.

Case No. 20-cr-188 (JSR)

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT RUBEN WEIGAND'S MOTION TO SUPPRESS EVIDENCE OBTAINED FROM THE SEARCH OF ELECTRONIC DEVICES

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

PRELIMINARY STATEMENT

By this motion, defendant Ruben Weigand ("Weigand") seeks to suppress evidence unlawfully seized by the Government from two cell phones and a computer (the "Devices") Weigand had with him at the time of his arrest. Remarkably, the Government's application for a warrant to search the Devices did not even purport to establish that those Devices had ever been used in, or had any connection whatsoever to, the alleged bank fraud scheme. Moreover, the Indictment itself alleges that the scheme had ended almost a year before the warrant was issued. Given the ubiquitous use of cell phones and computers, warrants to search electronic devices are, of course, commonplace, but that does not mean the Fourth Amendment's core protections do not apply. On the contrary, the applications for those warrants at least attempt to explain how the electronic devices to be searched were used to engage in criminal activity. The warrant application in this case makes absolutely no effort to do so.

The warrant application does describe a handful of electronic communications between Weigand and the Government's cooperating witness *from almost two years earlier* but nowhere does the Government assert that Weigand used the Devices to engage in those communications; in fact, there is no mention of any phone number or email account associated with Weigand. Instead of the required particularity, the Government resorted to dangerously broad assertions such as: "individuals engaged in criminal activity often store records of criminal activity" on their devices and "[l]ike individuals engaged in any other kind of activity, individuals who engage in fraud . . . store records relating to their illegal activity . . . on electronic devices."

These assumptions do not begin to satisfy the particularized evidence standards undergirding the Fourth Amendment. In order to search devices, the Government must explain,

at a bare minimum, why there is probable cause to believe that the particular devices it seeks to search may contain evidence of criminal activity at the time of the search.

In addition, the scope of the warrant itself is so broad that it authorizes the Government to scour the entirety of the data on the Devices, without limitation, and, for some categories of data described in the warrant, to do so without any temporal limitation. But, on the Government's own version of events, Weigand had no involvement whatsoever until January 2018 and the scheme ended in mid-2019. This overbroad warrant thus resulted in the Government seizing and producing in discovery over 300,000 files from Weigand's laptop, some dating back to as early as 2008—a full decade before the beginning of Weigand's alleged involvement in the scheme. The laptop contained thousands of documents stored in folders that were, on their face, not related to the alleged scheme. This includes, for example, thousands of photographs of family and friends and items stored in a folder marked "private." As the Government was no doubt aware, Weigand is a successful businessman involved in many lawful ventures having nothing at all to do with the allegations in this case, yet the application made no effort whatsoever to focus only on electronic data that pertains to the scheme described in the Indictment. The Government's production of documents from Weigand's laptop includes numerous documents that had been stored in folders making clear that the items related to business that had no connection whatsoever to the alleged scheme. And, all of these materials were apparently deemed responsive to the warrant after the Government conducted what it refers to in its cover letter producing the materials as "forensic analyses" of the Devices. The excessive sweep of the Government's collection and production confirms that the intrusive warrant was unconstitutionally overbroad.

Any evidence obtained through the unlawful searches of Weigand's electronic devices and the fruits thereof must be suppressed.

BACKGROUND

On March 9, 2020, Weigand was arrested at the Los Angeles International Airport in California, as he waited for a connecting flight for a vacation trip to Costa Rica. At that time, the Government seized a "black/dark grey OnePlus cell phone," a "silver MacBook Pro Model A1502," and a "black/dark grey Apple iPhone." Exhibit A, Agent Affidavit in Support of Application for Search and Seizure Warrant dated April 14, 2020 (the "Affidavit") at ¶ 3.

On April 14, 2020, Special Agent Matthew Mahaffey of the Federal Bureau of Investigation submitted an application for a search and seizure warrant as well as the accompanying Affidavit in support of the application.

The Affidavit provides an overview of the "Transaction Laundering Scheme," which was described in superseding indictment S3 20 Cr. 188 against Weigand and his co-defendant Ray Akhavan (the "Indictment"), and allegedly involved credit card transactions for a marijuana delivery company. Like the Indictment, the Affidavit alleges that "Weigand and Akhavan, working with others, including principals from [marijuana delivery company], one of the leading on-demand marijuana delivery companies in the United States, planned and executed a scheme to deceive United States banks and other financial institutions into processing over one hundred million dollars in credit and debit card payments for the purchase and delivery of marijuana products." *Id.* at ¶ 9. The Affidavit alleges that, to effectuate the scheme, Weigand and others "arranged for the money received from [the marijuana delivery company's] customers to be disguised as payments to over a dozen phony online merchants and other non-marijuana businesses," which "Weigand, Akhavan, and others, worked with other co-conspirators to create. . . ." *Id.* at ¶ 11. The Affidavit acknowledges that the alleged scheme would not have extended beyond "mid-2019," because "[the marijuana delivery company] stopped processing credit card

transactions in approximately mid-2019." *Id.* at ¶ 12. In the Affidavit, the agent claimed there was probable cause that the Devices contained "evidence, fruits, and instrumentalities" of —"bank fraud, and money laundering, in violation of Title 18, United States Code, Sections 1344 (bank fraud), 1349 (conspiracy to commit bank fraud), 1956 (money laundering), 1957 (engaging in monetary transactions in property derived from specified unlawful activity), and 1956(h) (conspiracy to commit money laundering)" (the "Subject Offenses"). *Id.* at ¶ 7.

The Affidavit does not assert that the Devices were used in connection with, or to communicate about, the alleged scheme. Nor does the Affidavit set forth that Weigand ever used any particular Device, phone number, or account, to conduct or communicate about the alleged scheme or to store records related to it, or for any other purpose. *Id.* at ¶ 16.

The Affidavit relies on four excerpts of group chats from almost two years before the Affidavit was submitted, purportedly involving Weigand, three of which involve the Government's cooperating witness. The chats are dated April 27, 2018 and July 31, 2018 and, according to the Affidavit, include discussion of the so-called "phony merchants." *Id.* at ¶¶ 17–18. The Affidavit provides no information about the devices, accounts, email addresses, or applications used to engage in these communications. In addition, the Affidavit refers to a January 17, 2018 meeting in Calabasas, California, at which Weigand, Akhavan, and others allegedly discussed the Transaction Laundering Scheme. *Id.* at ¶ 19(a). The Affidavit does not assert that any of the Devices were used at that meeting or that Weigand possessed the Devices at the meeting.

The Affidavit also contends, based on the agent's discussions with the Government's cooperating witness and his "review of a recording of a phone call," that Weigand communicated with the cooperating witness "as recently as in or around May 2019." *Id.* at ¶ 21. The Affidavit, however, does not assert that Weigand used either of the two seized phones when he participated

in the call. Moreover, the agent does not and cannot allege that this call was in furtherance of an ongoing crime.[1]

Instead of providing any particulars about the Devices to be searched, the Affidavit offers the general observation that "[l]ike individuals engaged in any other kind of activity, individuals who engage in fraud and money laundering offenses store records relating to their illegal activity and to persons involved with them in that activity on electronic devices such as the [Devices]." *Id.* at ¶ 22. The Affidavit adds, again in generic terms, that "[i]ndividuals engaged in criminal activity often store such records in order to, among other things, (1) keep track of co-conspirator's [sic] contact information; (2) keep a record of illegal transactions for future reference; and (3) keep an accounting of illegal proceeds for purposes of, among other things, dividing those proceeds with co-conspirators." *Id.* Nowhere does the Affidavit describe how Weigand allegedly used any electronic device—let alone any of the three seized devices—to store records of illegal activity. And, although the first indication the Affidavit offers of Weigand's involvement in the scheme concerns a meeting in January 2018, the warrant the Government requested sought many categories of data for the period 2016-2019 and, for some categories, sought data with no temporal limitation at all. The Affidavit's description of the January 2018 meeting also strongly suggests that the alleged scheme did not exist at all prior to the meeting. *Id*. at ¶ 19 (explaining how the meeting's attendees discussed, *inter alia*, "how the Transaction Laundering Scheme *would* work," that transactions "*were going to be* processed through the [p]hony [m]erchants," and "how the payment processing *would* work.") (emphasis added). Moreover, besides the Affidavit's

[1] The substance of this call was addressed at the April 24, 2020, bail hearing. As Weigand's counsel pointed out in the bail hearing, on this call, Weigand tells the cooperator that: "I'm not personally involved." April 24, 2020 Bail Hearing Transcript at 7:1–2. There is nothing in the call to indicate any ongoing involvement.

conclusory claim that the alleged scheme lasted from 2016-2019, the Affidavit offers no substantive evidence that the alleged scheme, in fact, began or was in operation at any point prior to the January 2018 meeting.

On the basis of the Affidavit, the Honorable U.S. Magistrate Judge Katharine H. Parker granted the Government's application for a warrant to search the Devices for sweeping amounts of information. *See* Exhibit B, Search and Seizure Warrant dated April 14, 2020 (the "Warrant"). The authorized categories are framed broadly and include, *inter alia*, "[e]vidence of the relationship between suspects, co-conspirators, and/or victims involved in the Subject Offenses" (Category 4), and "[e]vidence concerning financial transactions conducted by or between the co-conspirators and/or victims of the Subject Offenses" (Category 5). *Id*., Attachment A at 2–3. Since neither the Affidavit nor the Indictment identify any specific victims or suspects, but rather broadly allude to unnamed banks, these categories would seemingly include Weigand's personal credit card statements, including from years before he is alleged to have joined the conspiracy. Moreover, certain of the authorized categories have no discernible connection to the alleged scheme and the "Subject Offenses": they include "[n]on-content transactional information of activity of the [Devices]" (Category 8) and "[s]ubscriber information, in any form kept, pertaining to the [Devices]" (Category 9). *Id.* at 3. In addition, most of the categories listed in the Warrant contain no temporal restriction that would confine the Government's search to the timeframe of the alleged scheme. *See id*., Categories 1, 6-9 (providing no date range limitation).

The Warrant included no restrictions as to what data the Government could search through and review to find evidence responsive to the above categories—a proverbial "blank check" to review all data on the Devices. The Affidavit made abundantly clear that rummaging through every piece of data on the Devices is precisely what the Government intended to do—and did. The

Affidavit states that, ". . . law enforcement may need to conduct a complete review of all the [electronically stored information] from the [Devices] to locate all data responsive to the warrant." Ex. A, Affidavit at ¶ 27.

The Government, after having conducted what the discovery production cover letter refers to as "forensic analyses," presumably for the purpose of isolating materials responsive to the warrant, then produced in discovery 336,783 files, some of the materials dating back as far as 2008.[2] A cursory review of documents from outside the relevant period reveals a trove of personal data including thousands of pictures, a great deal of which are of friends and family. Even within the 2016-2019 time frame, the laptop contains personal files and non-related business files stored in folders with conspicuous names that indicate that they had no relation to the alleged scheme. This includes thousands of photographs from vacations and other personal affairs in folders labeled, for example, "Namibia," which contained thousands of photographs of a trip to Southern Africa, and "Olympus," which is named after a well-known camera company and similarly contained thousands of photographs of private moments with family and friends. It also included a folder named, simply, "private." The laptop also contained folders named after businesses that have no connection whatsoever to the alleged scheme.

[2] On May 12, 2020, the Government produced a USB drive to Weigand that, according to an accompanying cover letter, "contain[ed] the results of forensic analyses performed on several devices seized from the defendant pursuant to his arrest." Exhibit C, Government Production Cover Letter dated May 12, 2020; *see also United States v. Mutschelknaus*, 564 F. Supp. 2d 1072, 1076 (D.N.D. 2008) (referring to "forensic analysis" as the "subsequent search" that is performed on an electronic device after it has been seized).

LEGAL STANDARD

The Fourth Amendment mandates that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Thus, the Fourth Amendment provides two distinct protections—(1) the requirement that a warrant be issued upon a finding of probable case, and (2) that the warrant be particularly tailored based upon the probable cause established. The probable cause requirement recognizes that "any intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (citations omitted). The particularity requirement recognizes that, even where probable cause is established, still "those searches deemed necessary should be as limited as possible," as to avoid a "'general warrant,'" *i.e.*, "a general, exploratory rummaging in a person's belongings." *Id*. (citations omitted).

Given the considerable volume of personal, intimate, and private information that personal electronic devices can contain, the Supreme Court, and the Second Circuit, have recognized that the Fourth Amendment's privacy protections are particularly important in connection with searches of electronic data. *See Riley v. California*, 573 U.S. 373, 394 (2014) (noting that "a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record," and that "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions[.]"); *see also United States v. Galpin*, 720 F.3d 436, 446-47 (2d Cir. 2013) ("[A]dvances in technology and the centrality of computers in the lives of

average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain," and "[t]here is, thus, a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.") (citations and quotations omitted). The Supreme Court has recently recognized that even time-stamped location data kept by cell phone companies warrants Fourth Amendment protection given that the "data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (citing *United States. v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

ARGUMENT

I. THE WARRANT FAILS TO ESTABLISH PROBABLE CAUSE THAT THE DEVICES WERE USED IN CONNECTION WITH THE SUBJECT OFFENSES

A search warrant application purporting to establish that an individual has engaged in criminal activity does not establish probable cause to search the *entirety* of that individual's possessions. *See United States v. Pabon*, 871 F.3d 164, 181 (2d Cir. 2017), *cert. denied*, 139 S. Ct. 61 (2018) ("[A] determination of probable cause to search is not the same as a determination that there is, at the same time, probable cause to arrest, or vice versa."). Instead, a warrant to search a particular place must be supported by probable cause showing that there is a "fair probability that contraband or evidence of a crime will be found *in a particular place*." *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (emphasis added). Specifically, the Fourth Amendment demands "a sufficient nexus between the criminal activities alleged" and the location or items searched. *United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004). With respect to the evidence used to establish probable cause, "the proof must be of facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause at that time." *Sgro v. United States*, 287 U.S.

206, 210 (1932); *see also United States v. Wagner*, 989 F.2d 69, 75 (2d Cir. 1993) (no probable cause existed where affidavit relied on marijuana purchase six weeks prior to issuance of the warrant). Those principles apply with equal force to searches of electronic devices. Indeed, given the ubiquitous use of those devices in modern society it is all the more important to insist that the Government turn square corners under the Fourth Amendment. *See*, *e.g.*, *Riley*, 573 U.S. at 394.

A. The Affidavit Does Not Purport To Claim That The Devices Had Any Connection To The Alleged Criminal Conduct And Relies On Stale Evidence

The Affidavit does not include any assertion that Weigand actually used the Devices in connection with the offenses described in the search warrant Affidavit. Unlike cases where courts have upheld broad search and seizure warrants for electronic devices, the Affidavit in this case provided no evidence that calls, text messages, or emails regarding the scheme described in the Affidavit were sent or received from the Devices, or that records related to the scheme were kept on the Devices. *See, e.g., United States v. Gatto*, 313 F. Supp. 3d 551, 554 (S.D.N.Y. 2018) (upholding validity of cell phone warrants where the warrant applications were supported by wiretap evidence demonstrating that the electronic devices were used to communicate about the subject offenses). Nor were the Devices in this case seized from Weigand while he was conducting activity in furtherance of the Subject Offenses. *See id.* (upholding validity of cell phone warrants where, at the time of the defendant's arrest, the defendant had cell phone on his person while en route to meet an undercover FBI agent to discuss subject offenses); *see also United States v. Ulbricht*, 858 F.3d 71, 86 (2d Cir. 2017), *cert. denied*, 138 S. Ct. 2708 (2018) (upholding laptop warrant where, at the time of the defendant's arrest, the defendant's laptop was open and the defendant was conducting activities in furtherance of the subject offenses via his laptop).

The Affidavit fails to link the handful of electronic communications it does describe with the Devices. Notably, those communications were almost two years old when the Devices were

seized. *See* Ex. A, Affidavit at ¶¶ 17-18 (quoting excerpts of encrypted chats—three of which were from April 27, 2018 and the most recent of which was from July 31, 2018). Further, the most recent communication the Affidavit cites is a phone call between Weigand and the cooperating witness in May 2019. *Id*. at ¶ 21. The Affidavit, however, does not say which phone or phone number was used by Weigand to make the call. Nor can or does the agent claim that the call was part of the alleged conspiracy. The considerable passage of time between the communications cited in the Affidavit and the issuance of the warrant rendered the evidence stale and insufficient to establish probable cause that evidence of the Subject Offenses would be found on the Devices. *See United States v. Thomas*, 757 F.2d 1359, 1368 (2d Cir. 1985) (holding that "two-year-old evidence of participation in a heroin mill, *not* at the dwelling to be searched, is stale and cannot support a search warrant") (emphasis in original).

B. The Affidavit's Generic And Irrelevant Assertions That Criminals Store Evidence Of Their Crimes On Electronic Devices Does Not Amount To Probable Cause To Search The Devices

In a flawed effort to overcome the Affidavit's failure to connect the Devices to the Subject Offenses, the Affidavit resorts to vague, general assertions that amount to nothing more than the irrelevant observation that people who commit crimes—and those who do not—use electronic devices. The affidavit states that: "*Like individuals engaged in any other kind of activity*, individuals who engage in fraud and money laundering offenses store records relating to their illegal activity and to persons involved with them in that activity on electronic devices such as the [Devices]." Ex. A, Affidavit at ¶ 22 (emphasis added). The Affidavit adds, again in generic terms, that "[i]ndividuals engaged in criminal activity often store such records in order to, among other things, (1) keep track of co-conspirator's [sic] contact information; (2) keep a record of illegal transactions for future reference; and (3) keep an accounting of illegal proceeds for purposes of, among other things, dividing those proceeds with co-conspirators." *Id*.

Such generalized statements do not comport with the legal standards applicable to searches and seizures. *See, e.g., United States v. Brown*, 828 F.3d 375, 383 (6th Cir. 2016) ("We have never held . . . that a suspect's 'status as a drug dealer, standing alone, gives rise to a fair probability that drugs will be found in his home'. . . [r]ather, we have required some reliable evidence connecting the known drug dealer's ongoing criminal activity to the residence; that is, *we have required facts showing that the residence had been used in drug trafficking*, such as an informant who observed drug deals or drug paraphernalia in or around the residence.") (emphasis added and citations omitted); *see also United States v. Kortright*, No. 10 Cr. 937 (KMW), 2011 WL 4406352, at *7 (S.D.N.Y. Sept. 13, 2011) (finding no probable cause to search defendant's residence based on agent's opinion that drug traffickers commonly store contraband at their residence). The Fourth Amendment demands more—an application for a search warrant must establish a "sufficient nexus" between the place to be searched and the evidence to be sought. *Singh*, 390 F.3d at 182; *see also United States v. Frazier*, 423 F.3d 526, 531-532 (6th Cir. 2005) (probable cause not established where informants had not "witnessed [the defendant] dealing drugs from his [new] residence," just his old residence); *United States v. Guzman*, No. S5 97 CR 786 (SAS), 1998 WL 61850, at *4 (S.D.N.Y. Feb. 13, 1998) ("Permitting 'a search warrant based solely on the self-avowed expertise of a law-enforcement agent, without any other factual nexus to the subject property, would be an open invitation to vague warrants authorizing virtually automatic searches of any property used by a criminal suspect.'") (quoting *United States v. Rosario*, 918 F. Supp. 524, 531 (D.R.I. 1996)).

Furthermore, the Government's Affidavit ignores the heightened protection that courts have recognized must be applied in the context of searches of electronic devices in this day and age since so much personal information is stored on electronic devices. *See*, *e.g.*, *United States v.*

Ganias, 755 F.3d 125, 135 (2d Cir. 2014), *rev'd en banc on other grounds*, 824 F.3d 199 (2d Cir. 2016) ("The[] Fourth Amendment protections apply to modern computer files. Like 18th Century 'papers,' computer files may contain intimate details regarding an individual's thoughts, beliefs, and lifestyle, and they should be similarly guarded against unwarranted Government intrusion. If anything, even greater protection is warranted.") (citation omitted).

II. THE WARRANT IS OVERBROAD BECAUSE IT FAILS TO LIMIT THE SCOPE OF THE SEARCH AND PROVIDES NO MEANINGFUL GUIDANCE AS TO THE CONTENT TO BE SEIZED

The evidence obtained from the Devices should also be suppressed because the Warrant permitted an unconstitutionally overbroad search of the Devices. The Warrant made no attempt to limit the scope of the search to the locations on the Devices for which there was probable cause to believe evidence of the scheme could be found. *See Maryland v. Garrison*, 480 U.S. 79, 84 (1987) ("By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the [Fourth Amendment] ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.") (footnote omitted). It did not require the Government, for example, to look at the titles of the folders containing data, to determine if there was probable cause to believe each folder contained evidence of a crime, or, alternatively, contained family photos, medical records or documents related to businesses with no connection to the charged scheme.

Moreover, the Warrant did not limit in any meaningful way what items could be seized from the Devices, amounting to an impermissible general warrant. While the scope of the Warrant purports to be limited to certain categories of materials, the limitation is entirely illusory. The vague, catch-all language of those categories, authorized the search and seizure of *any* data on the Devices. *See United States v. Wey*, 256 F. Supp. 3d 355, 382 (S.D.N.Y. 2017) ("The doctrine of overbreadth represents, in a sense, an intersection point for probable cause and particularity

principles: it recognizes, in pertinent part, that a warrant's unparticularized description of the items subject to seizure may cause it to exceed the scope of otherwise duly established probable cause.")

A. The Warrant Permitted The Government To Conduct Sweeping Searches Of All Data Contained On The Devices

The Affidavit listed several exhaustive techniques the Government planned to use to review the contents of the Devices. This included, "'scanning' storage areas to discover and possibly recover recently deleted data[,] scanning storage areas for deliberately hidden files[,]" "surveying directories or folders and the individual files they contain[,]" and "conducting a file-by-file review by 'opening' or reading the first few 'pages' of such files in order to determine their precise contents." Ex. A, Affidavit at ¶ 26. And, if the combination of the above 'no stone unturned' techniques did not sufficiently demonstrate the Government's intention to search the entire contents of the Devices, the Government removed any such ambiguity by reserving its right, "[d]epending on the circumstances, . . . to conduct a complete review of all the [electronically stored information] from the [Devices] to locate all data responsive to the warrant." *Id*. at ¶ 27. The Warrant contained no restrictions on the places on the Devices the Government could search or the type of electronic data (*e.g.*, messages, videos, photos, etc.) that the Government could review. Moreover, the Affidavit, in detailing the boundless search the Government planned to execute, failed to identify any procedures the Government would follow to protect the inadvertent review of privileged communications. Such an absolute, limitless search was not justified based on the evidence in the Affidavit, the general representations regarding criminals' use of electronic devices, or the nature of the crime alleged.

Based on what was produced in discovery, which included thousands of personal photos, it appears that, in fact, the vast majority of the data that resulted from the Government's "forensic analyses" of the Devices had no relationship to the scheme or to any business whatsoever. Ex. C,

Gov. Production Letter. Further, the discovery also included vast amounts of data concerning lawful business ventures unrelated to the alleged scheme or any co-conspirators that the Government has identified.

B. The Warrant Provided No Meaningful Guidelines As To What Data Fell Within The Purview Of The Warrant

The Warrant also failed to establish any meaningful guidance or restrictions on what "data" was, indeed, "responsive to the warrant." Ex. A, Affidavit at ¶ 27. The Warrant listed nine categories of data that the Government was permitted to seize. Some of the categories had no date limitation at all. *See* Ex. B, Warrant, Attachment A at 2-3 (Categories 1, 6-9) (providing no date range limitation). The combination of these categories, and their broad, catch-all language, left no data outside the scope of the Warrant. *See United States v. George*, 975 F.2d 72, 75 (2d Cir. 1992) ("The instant warrant's broad authorization to search for 'any other evidence relating to the commission of a crime' plainly is not sufficiently particular with respect to the things to be seized because it effectively granted the executing officers' virtually unfettered discretion to seize anything they [saw].") (citations and quotations marks omitted).

Category 3 of the Warrant permitted the Government to search any "*stored content information* presently contained in, or on behalf of, the Devices, covering the time period of 2016 to 2019[.]" Ex. B, Warrant, Attachment A at 2 (emphasis added). In other words, it authorized the search of all data on the Devices, without regard to whether the data was contained in folders indicating the material to be purely personal or irrelevant.

Category 4 of the Warrant authorized the Government to search for "[e]vidence of the relationships between suspects, co-conspirators, and/or victims involved in the Subject Offenses, covering the time period of 2016 to 2019[.]" *Id*. at 3. Permitting the Government to search for "[e]vidence of the relationships" between unidentified "suspects" and "victims" gives the

Government unbridled discretion. Conceivably, with the identity of "suspects" and "victims" left to the sole discretion of the Government, the Warrant gives the Government the authority to search for and seize any data on the Devices involving any individual. *See United States v. Zemlyansky*, 945 F. Supp. 2d 438, 459 (S.D.N.Y. 2013) (finding warrant lacked particularity where several of the warrant's categories "suffer[ed] from ambiguity" and could give executing officers "extremely broad discretion in deciding what items" fell within their scope).

Further, with respect to some of the categories, the Warrant fails to connect the pertinent data with the Subject Offenses. For example, Category 8 permits the Government to search for "[n]on-content transactional information of activity of the [Devices], including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations[.]" Ex. B, Warrant, Attachment A at 3. Category 9 permits the Government to search for "[s]ubscriber information, in any form kept, pertaining to the [Devices], including, but not limited to, applications, subscribers' full names, all user names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records." *Id*. Neither Category 8 nor Category 9 is limited to data within those categories that is related, in any way, to the Subject Offenses or to the relevant time period.

Moreover, although the Affidavit speaks to a scheme lasting from 2016 to 2019, the Affidavit provides no evidence that Weigand was involved prior to the January 17, 2018 meeting in Calabasas, California. *See* Ex. A, Affidavit at ¶ 19. In fact, the very description of the meeting in the Affidavit indicates that the alleged scheme, *i.e.*, the "Transaction Laundering Scheme," did not exist prior to the January 2018 meeting. The Affidavit states that, at the meeting, the attendees discussed: (1) "how the Transaction Laundering Scheme *would* work," (2) "the underlying transactions that *were* going to be processed," and (3) "how the payment processing *would* work."

Id. Thus, the Affidavit failed to establish any probable cause that would justify the Warrant's authorization to search and seize data prior to 2018.

Courts have invalidated warrants permitting such broad seizures of electronic data. For example, in *United States v. Winn*, which District Judge Alison J. Nathan of this Court recently cited in a decision granting a motion to suppress, the warrant at issue authorized the seizure of "'any or all files' contained on the cell phone and its memory card that 'constitute[d] evidence of the offense of [Public Indecency 720 ILCS 5/11–30],' including, but not limited to, the calendar, phonebook, contacts, SMS messages, MMS messages, emails, pictures, videos, images, ringtones, audio files, all call logs, installed application data, GPS information, WIFI information, internet history and usage, any system files, and any delated data." 79 F. Supp. 3d 904, 919 (S.D. Ill. 2015) (footnote and citation omitted); *see also Wey*, 256 F. Supp. 3d at 392 (Nathan, J., citing *Winn*). The *Winn* court invalidated the warrant, finding that the "major, overriding problem" with the object of the search covering "any or all files" that constitute evidence of public indecency was that the "police did not have probable cause to believe that *everything* on the phone was evidence of the crime of public indecency." *Winn*, 79 F. Supp. at 919 (emphasis in original and quotation marks omitted). As the *Winn* court held, "if [the officer] wanted to seize every type of data from the cell phone, then it was incumbent upon him to explain . . . how and why each type of data was connected to [the defendant's] criminal activity, and he did not do so." *Id*. at 920.

As in *Winn*, the Warrant in this case granted the Government unfettered authorization to "rummage through every conceivable bit of data" on the Devices. *Winn*, 79 F. Supp. at 922. There was no probable cause to believe the Devices had any connection to the charged scheme, no reason to believe that the vast amount of materials, particularly materials from the years other than 2018-2019, would be related to the Subject Offenses.

III. ALL EVIDENCE DERIVED FROM THE UNLAWFUL SEARCH OF THE DEVICES MUST BE SUPPRESSED

The Government cannot rely on the good faith exception to save the otherwise invalid Warrant because reliance on the Warrant would not have been objectively reasonable. *See George*, 975 F.2d at 77 (In determining whether the good faith exception applies, "[t]he burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance" on an invalidated warrant.) (citation omitted). First, because the Affidavit failed to link the Devices to the Subject Offenses, and relied on stale evidence, the Affidavit was "so lacking in indicia of probable cause" for the search of the Devices that "reliance upon it [was] unreasonable." *Wey*, 256 F. Supp. 3d at 395. Second, because the Warrant authorized a limitless search of all the data on the Devices, and authorized the seizure of expansive categories of data with no meaningful restrictions, guidelines, or connection to the Subject Offenses, the Warrant was "so facially deficient that reliance upon it [was] unreasonable." *Id.* (quotation marks and citation omitted)

The Affidavit did not establish probable cause that Weigand used the Devices in connection with the Subject Offenses or that any evidence would have been retained on the Devices at the time the Affidavit was submitted when the Affidavit itself asserts that, the alleged scheme ended in mid-2019. Ex. A, Affidavit at ¶ 12. Further, although the Affidavit provided outdated excerpts from 2018 of group chats purportedly involving Weigand, the Affidavit failed to establish probable cause that there would be evidence of the Subject Offenses in the vast troves of non-communication data that the Affidavit requested to search and seize (*e.g.*, videos, images, photos, information concerning social media accounts, "other stored content," "[n]on-content transactional information," etc.). Ex. B, Warrant, Attachment A at 2–3.

Aside from the deficiencies in the Affidavit itself, the Warrant was so facially overbroad that no officer could have reasonably believed that it was valid under the Fourth Amendment. *See*

Wey, 256 F. Supp. 3d at 398 (finding suppression appropriate where warrants "authorize[d] the seizure of multiple expansive categories of records (*e.g.*, 'notes,' 'memoranda,' 'correspondence,' 'communications,' 'photographs,' etc.) without any meaningful linkage to the suspected criminal conduct"); *see also United States v. Leary*, 846 F.2d 592, 609 (10th Cir. 1988) ("A reasonably well-trained officer should know that a warrant must provide guidelines for determining what evidence may be seized.")

It is not objectively reasonable for an executing officer to rely on a warrant that allows the executing officer to search and seize all conceivable data on an electronic device, as is the case here. *See Winn*, 79 F. Supp. 3d at 924 (holding that the good faith exception was not applicable to save an invalid cell phone warrant because "it was not objectively reasonable for [the executing officers] to think that a warrant was valid when it gave them unbridled discretion to search for and seize whatever they wished"). Nor is it objectionably reasonable to rely on a warrant to search, endlessly, through three electronic devices belonging to an individual engaged in many legitimate business ventures, with no guidelines or procedures to limit the inadvertent review of privileged communications or business documents unrelated to the alleged scheme.

CONCLUSION

For the foregoing reasons, Defendant Ruben Weigand respectfully requests that the Court suppress all evidence obtained from the searches of the Devices.

Dated: New York, New York
June 26, 2020

Respectfully submitted,

DECHERT LLP

By: */s/ Andrew J. Levander*

Andrew J. Levander
Michael J. Gilbert
Shriram Harid
Steven Pellechi
Three Bryant Park
1095 Avenue of the Americas
New York, New York 10036-6797
Andrew.levander@dechert.com
Michael.gilbert@dechert.com
Shriram.harid@dechert.com
Steven.pellechi@dechert.com

Michael H. Artan
Michael H. Artan, Lawyer, A Professional Corporation
1 Wilshire Boulevard, Suite 2200
Los Angeles, CA 90071
Michaelartan@yahoo.com

Attorneys for Defendant
Ruben Weigand